European Journal of Combinatorics 47 (2015) 1–14

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Systems of word equations, polynomials and linear algebra: A new approach

Aleksi Saarela

Department of Mathematics and Statistics, University of Turku, FI-20014 Turku, Finland

ARTICLE INFO

Article history:
Received 10 October 2013
Accepted 9 January 2015
Available online 4 February 2015

ABSTRACT

We develop a new tool, namely polynomial and linear algebraic methods, for studying systems of word equations. We illustrate its usefulness by giving essentially simpler proofs of several hard problems. At the same time we prove extensions of these results. Finally, we obtain the first nontrivial upper bounds for the fundamental problem of the maximal size of independent systems. These bounds depend quadratically on the size of the shortest equation. No methods of having such bounds have been known before.

1. Introduction

Combinatorics on words is a part of discrete mathematics. It studies the properties of strings of symbols and has applications in many areas from pure mathematics to computer science. See, e.g., [23] or [3] for a general reference on this subject.

Some of the most fundamental questions in combinatorics on words concern word equations. First such question is the complexity of the satisfiability problem, i.e., the problem of determining whether a given equation with constants has a solution. The satisfiability problem was proved to be decidable by Makanin [24] and proved to be in PSPACE by Plandowski [27], and it has been conjectured to be NP-complete.

A second question is how to represent all solutions of a constant-free equation. Hmelevskiĭ proved that the solutions of an equation on three unknowns can be represented with parametric words, but this does not hold for four unknowns [13]. The original proof has been simplified [19] and used to study a special case of the satisfiability problem [28].

E-mail address: amsaar@utu.fi.

http://dx.doi.org/10.1016/j.ejc.2015.01.005
0195-6698/

A third fundamental question, which is very important for this article, is the maximal size of an independent system of word equations. It was proved by Albert and Lawrence [1] and independently by Guba [9] that an independent system cannot be infinite. However, it is still not known whether there are unboundedly large independent systems.

One of the basic results in the theory of word equations is that a nontrivial equation causes a defect effect. In other words, if n words satisfy a nontrivial relation, then they can be represented as products of $n-1$ words. Not much is known about the additional restrictions caused by several independent relations [10].

In fact, even the following simple question, formulated already in [4], is still unanswered: How large can an independent system of word equations on three unknowns be? The largest known examples consist of three equations. This question can be obviously asked also in the case of $n > 3$ unknowns. Then there are independent systems of size $\Theta(n^4)$ [18]. Some results concerning independent systems on three unknowns can be found in [12,6,7], but the open problem seems to be very difficult to approach with current techniques.

There are many variations of the above question: We may study it in the free semigroup, i.e., require that $h(x) \neq \varepsilon$ for every solution h and unknown x, or examine only the systems having a solution of rank $n-1$, or study chains of solution sets instead of independent systems. See, e.g., [11,10,5,20].

In this article we will use polynomials to study some questions related to systems of word equations. Algebraic techniques have been used before, most notably in the proof of Ehrenfeucht's conjecture, which is based on Hilbert's basis theorem. However, the way in which we use polynomials is quite different and allows us to apply linear algebra to the problems.

The main contribution of this article is the development of new methods for attacking problems on word equations. This is done in Sections 3 and 5. Other contributions include simplified proofs and generalizations for old results in Sections 4 and 6, and studying maximal sizes of independent systems of equations in Section 6. Thus the connection between word equations and linear algebra is not only theoretically interesting, but is also shown to be very useful at establishing simple-looking results that have been previously unknown, or that have had only very complicated proofs. In addition to the results of the paper, we believe that the techniques may be useful in further analysis of word equations.

Next we give a brief overview of the paper. First, in Section 2 we define a way to transform words into polynomials and prove some basic results using these polynomials.

In Section 3 we prove that if the lengths of the unknowns are fixed, then there is a connection between the ranks of solutions of a system of equations and the rank of a certain polynomial matrix. This theorem is very important for all the later results.

Section 4 contains small generalizations of two earlier results. These are nice examples of the methods developed in Section 3 and have independent interest, but they are not important for the later sections.

In Section 5 we analyze the results of Section 3 when the lengths of the unknowns are not fixed. For every solution these lengths form an n-dimensional vector, called the *length type* of the solution. We prove that the length types of all solutions of rank $n-1$ of a pair of equations are covered by a finite union of $(n-1)$-dimensional subspaces if the equations are not equivalent on solutions of rank $n-1$. This means that the solution sets of pairs of equations are in some sense more structured than the solution sets of single equations. This theorem is the key to proving the remaining results.

We begin Section 6 by proving a theorem about unbalanced equations. This gives a considerably simpler reproof and a generalization of a result in [12]. Finally, we return to the question about sizes of independent systems. There is a trivial bound for the size of a system depending on the length of the longest equation, because there are only exponentially many equations of a fixed length. We prove that if the system is independent even when considering only solutions of rank $n-1$, then there is an upper bound for the size of the system depending quadratically on the length of the shortest equation. Even though it does not give a fixed bound even in the case of three unknowns, it is a first result of its type—hence opening, we hope, a new avenue for future research.